AUSA: Christopher Rawsthorne Telephone: (313) 226-9100

AO 91 (Rev. 11/11) Criminal Complaint Special Agent: Matthew Hughes Telephone: (313) 965-2323

UNITED STATES DISTRICT COURT

for the

Eastern District of Michigan

United States of America
v.
Dangelo Charles Mckenzie

Case No. Case: 2:23-mj-30095
Assigned To : Unassigned Assign. Date : 3/8/2023
USA V. MCKENZIE (CMP)(CMC)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July 2022 through March 8, 2023 in the county of Wayne and elsewhere in the Eastern District of Michigan, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 875(d)	Sending threatening communications
18 U.S.C. § 2261A(2)(B)	Online stalking
18 U.S.C. § 2252A(a)(2)	Receipt of child pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of child pornography

This criminal complaint is based on these facts:
see attached affidavit.

☑ Continued on the attached sheet.

Complainant's signature

Matthew R. Hughes, Special Agent (FBI)
Printed name and title

Sworn to before me and signed in my presence
and/or by reliable electronic means.

Date: March 8, 2023

Judge's signature

City and state: Detroit, Michigan

Hon. Anthony P. Patti, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Matthew Hughes, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the FBI since 2019 and am currently assigned to the Detroit Division. While employed by the FBI, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training and everyday work relating to conducting child exploitation investigations. To date, I have either conducted or participated in over 100 child exploitation investigations.

2. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 875, 1030, 2251, 2252A, 2261A, and 2422. I am authorized by law to request an arrest warrant.

3. This affidavit is submitted in support of an application for a criminal complaint and arrest warrant for Dangelo Charles Mckenzie for violations of 18 U.S.C. § 2252A(a)(2) (receipt of child pornography), 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), 18 U.S.C. §§ 875(d) (threatening

communications), and 2261A(2)(B) (online stalking).

4. The statements contained in this affidavit are based in part on information provided by U.S. law enforcement officers, written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from investigative sources of information, and my experience, training, and background as a Special Agent.

5. This affidavit is submitted for the limited purpose of securing an arrest warrant. I have not included every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish probable cause that Mckenzie has violated Title 18 U.S.C. §§ 2252A(a)(2), 2252A(a)(5)(B), 875(d) and 2261A(2)(B).

SUMMARY OF PROBABLE CAUSE

6. Mckenzie threatened to and did post and attempt to sell nude images of an adult victim, hereafter AV1. Mckenzie and AV1 do not appear to know each other personally, but I believe that Mckenzie was the individual who did this because 1) Records from Block, Inc. showed that a Cashapp username used by Mckenzie to attempt to sell images of AV1, $jupiterclouds, came back to Mckenzie's name with his date of birth; 2) Records from TextNow, a Voice Over Internet Protocol (VOIP) phone number provider, as well as from Comcast and AT&T, showed that the IP addresses used to log into VOIP telephone numbers used to communicate with AV1

resolved to Mckenzie's residence and to a recording studio that Mckenzie frequented; 3) Records from Google showed that the Google account used to create at least two of the VOIP phone number accounts, dopeasmoney@gmail.com, had billing information showing it was Mckenzie's account; 4) Records from Snapchat and TikTok showed that AV1's accounts had logins from the IP addresses shown to be used at Mckenzie's residence and the recording studio that he frequented; 5) Records from Meta, the owner of Instagram, showed that the same IP addresses associated with Mckenzie's residence and the recording studio that Mckenzie frequented were used to log in to an Instagram account, username lov3nicole, used to communicate with AV1 initially after her accounts were hacked . I have further outlined the underlying investigation that demonstrates these facts below.

PROBABLE CAUSE

7. On August 23, 2022, an adult victim, hereafter referred to as AV1, who resides in the Eastern District of Michigan and who was born in June 2004, contacted the FBI with information that over the past two months, someone had accessed her Snapchat accounts with username sxucyyan and sxucyyay. This person had contacted AV1 via text messages, through phone numbers, including (248) 599-****, and Instagram, with a username lov3nicole_, and showed that they were in possession of nude images of AV1 from when she was a minor. The individual threatened to post the images to social media sites unless AV1 sent money or more

nude images of herself.

8. On September 2, 2022, AV1 provided a screenshot of the messages she had received from Instagram account lov3nicole_. In the messages the user of the account states (all errors in original): "Some one is posting your nudes hun" then shared an image of AV1 with her breasts exposed. AV1 identified herself as being 17 years old in this image. The user of lov3nicole_ went on to say: "The page their posting in is a hacked Snapchat I know a girl who can help you." AV1 did not recall exactly when she had received these messages, but it had happened during July or August of 2022.

9. AV1 also provided screenshots of text messages she had received by an individual threatening to post her nude images. A screenshot of the text messages she exchanged with telephone number 248-599-****, on or about August 9, 2022, showed the following:

599: I don't want to expose you Please cooperate

599: Suit yourself i'll post everything

AV1: Cooperate with what you wanting to hack my snap?

599: I just want more. If you send them i'll leave you alone If not i will get or snapchat and Instagram and post them

AV1: posting non consensual pornography and child pornography is a felony

5999: I guess I have a felony then I'll hack you now

599: Smh Y'all always choose the hard way

AV1: Who's this?

599: It doesn't matter i'll ask one last time will you cooperate yes or no

10. On or about August 23, 2022, AV1 received messages from telephone number 770-353-**** stating, "I don't want to expose you if you cash app or chime me i'll delete everything; If not i'm taking your snapchat and posting everything". On or about September 1, 2022, AV1 received messages from telephone number 385-344-****, "Look I don't want to expose you; I just need to make some money; If you shut up and let me I'll stop hacking you; Just give the account back I'll give it back when I'm done; Or I can hack you and expose you; Your choice.; I warned you". AV1 then received a notification from Snapchat stating that an unknown device had logged into her Snapchat account with username sxucyyay.

11. AV1 also provided emails that she had received from Snapchat identifying new devices logging into her accounts. On August 1, 2022, she had received an email from Snapchat stating that a Moto G Power (2022) was logging into her account with username sxucyyan from IP address 73.145.246.40. On August 23, 2022, she had received an email from Snapchat stating that an iPhone 8 Plus was logging into her account with username sxucyyay from IP address 68.48.252.3. And, on September 4, 2022, she had received an email from Snapchat stating that an iPhone 8 Plus was logging into her account with username sxucyyay

from IP address 162.198.6.183.

12. I obtained a search AV1's Snapchat account and determined that at least one of the images that would have been obtained by Mckenzie through accessing her Snapchat account would meet the federal definition of child pornography.

13. On September 2, 2022, an administrative subpoena was served on Meta Platforms for the Instagram account with username lov3nicole_. On September 7, 2022, Meta returned information which showed the account had the account ID of 199819236. The return also showed that the IP addresses used to log into the account had all been owned by Comcast.

14. On September 8, 2022, after preserving the Instagram account with ID 199819236, a 2703(d) Court Order authorized in the Eastern District of Michigan was served on Meta Platforms for subscriber information, linked accounts, and chat transaction history of the account. On October 21, 2022, Meta Platforms returned information which showed the account had changed the username to youlov3nicole_. One of the linked accounts had the ID 1743869658 with display name "GoGood or NoGood," which is discussed further below. The chat transaction history showed the three messages sent to AV1 on August 8, 2022. There were other messages in the chat transaction history that are between the account and other females who appear to be in their late teens or early twenties based on an open-source review of their accounts.

15. On September 2, 2022, an administrative subpoena was served on TextNow, a Voice Over Internet Protocol (VOIP), telephone number provider, for the telephone number (248) 599-****. On September 12, 2022, TextNow returned information which showed the account utilizing the phone number during the time of the communication with AV1 had the username Dopeas Money and an associated email address of dopeasmoney@gmail.com.

16. On September 8, 2022, an administrative subpoena was served on Snapchat for the account of AV1 with username sxucyyay. On October 4, 2022, Snapchat returned information which showed that the phone number associated with the account had been changed from AV1's known phone number to the phone number (231) 559-**** on September 4, 2022. The logs also showed login from IP addresses 68.48.252.3 on August 23, 2022, 162.198.6.183 on September 2, 2022 and September 4, 2022.

17. On October 6, 2022, an administrative subpoena was served on TextNow for the telephone number (231) 559-****. On October 7, 2022, TextNow returned information which showed the account was in the name Dopeas Money and an associated email address of dopeasmoney@gmail.com.

18. On November 14, 2022, AV1 provided further information that in the early morning hours on that day, someone had gained unauthorized access to her Snapchat account with username sxucyyan and her TikTok account with username

sxucylingling. AV1 started to receive numerous phone calls and eventually received a text message from phone number (248) 900-**** which stated, "If you want me to stop then cash app me." The individual that had taken over her accounts then began to message contacts she had on the apps offering to sell them nude images of AV1 for $60 and provided a CashApp username of $jupiterclouds.

19. AV1 provided email notifications from Snapchat showing that a new device, again a Moto G Power (2022) was used to login to her account with username sxucyyan on November 14, 2022, from IP address 162.198.8.183.

20. On November 14, 2022, an administrative subpoena was served on Snapchat for the username sxucyyan. On November 14, 2022, Snapchat returned information which showed numerous logins to the account from IP address 162.198.8.183 on November 14, 2022.

21. On November 14, 2022, an administrative subpoena was served on TikTok for the username sxucylingling. On January 10, 2023, TikTok returned information which showed a signup device of a Moto G Power (2022) and logins from IP address 162.198.8.183 on November 14, 2022.

22. On November 14, 2022, an administrative subpoena was served on TextNow for phone number (248) 900-****. On November 18, 2022 TextNow returned information which showed an account in the name Dopeas Money and an associated email address of dopeasmoney@gmail.com which owned the phone

number from November 11, 2022 to November 15, 2022. The IP logs for the account showed numerous logins from IP address 162.198.8.183 between November 11, 2022 and November 15, 2022.

23. On November 14, 2022, an administrative subpoena was served on company Block for the Cash App username $jupiterclouds. On December 7, 2022, Block returned information which showed the account was associated with Dangelo Mckenzie, with date of birth in 2000. The phones used to login to the account included an iPhone from October 2 to October 21, 2022, and a Motorola Moto G Power 2022 from October 27 to November 14, 2022. The IP logs showed consistent logins to the account from IP address 162.198.6.183 from October 2 to November 14, 2022. There was one login from IP address 73.145.246.85 on October 27, 2022.

24. A check of Michigan Secretary of State information for Dangelo Mckenzie with date of birth in 2000, which matches the date of birth provided by the subpoena response from Block, revealed a record for Dangelo Charles Mckenzie Jr. with residence address listed at Address 1.

25. Over the course of the investigation, multiple administrative subpoenas were served on Google for the account associated with email address dopeasmoney@gmail.com. Google has returned information which showed that the account was associated with Dangelo Mckenzie. The IP logs showed many logins

from IP address 162.198.6.183 between September 2, 2022, and January 1, 2023. There were also logins from IP address 68.48.252.3 between August 9, 2022, and January 10, 2023. In addition, there was a login from IP address 2607:fb91:1119:4e87:1526:ce8c:7ee0:d632 on November 25, 2022 at 1:47 UTC.

26. Throughout the investigation, the IP address 68.48.252.3 was observed to be used to login to the accounts owned by AV1, the accounts used to communicate with her and the email address associated with Dangelo Mckenzie, dopeasmoney@gmail.com. An administrative subpoena to Comcast for the subscriber of this IP address returned information that the subscriber was Rashad Green on Hazelwood Street in Detroit, Michigan. Comcast also returned information regarding Xfinity WiFi IP addresses that were assigned to this account which included 73.145.246.40 on August 1, 2022, when it was used to log in to AV1's Snapchat account with username sxucyyan and 73.145.246.85 on October 27, 2022, when it was used to log in to the Cash App account $jupiterclouds.

27. Throughout the investigation, the IP address 162.198.6.183 was observed to be used to login to the accounts owned by AV1, the accounts used to communicate with her and the email address associated with Dangelo Mckenzie, dopeasmoney@gmail.com. An administrative subpoena to AT&T for the subscriber of this IP address returned information that the subscriber was Shaphan Williams on E 8 Mile Road in Warren, Michigan. Open-source information showed that this

address is a recording studio.

28. On December 13, 2022, an administrative subpoena was served on T-Mobile for the IP address 2607:fb91:1119:4e87:1526:ce8c:7ee0:d632 on November 25, 2022 at 1:47:26 UTC. On December 20, 2022, T-Mobile returned information that the phone number utilizing the IP address at the specified date and time was 313-912-****. On January 4, 2023, an administrative subpoena was served on T-Mobile for the telephone number 313-912-****. On January 4, 2023, T-Mobile returned information that the subscriber was Individual A, McKenzie's mother, at the residence in Detroit, Michigan That residence is the same address that the Comcast IP addresses came back to as described above.

29. The subpoena return information for (313) 912-7199 received on January 4, 2023, also included call detail records for the phone number. Analysis of these phone number showed that phone numbers associated with Individual A and Individual B (Mckenzie's stepfather) were two of the top ten most called numbers for the phone.

30. As described above, the 2703(d) Court Order for the Instagram Subject Account 199819236 showed a linked account with user ID 1743869658 and display name GoGood or NoGood. On October 24, 2022, an administrative subpoena to Meta for subscriber information for this linked account was served. On October 27, 2022, Meta returned information which showed the username as o0baby. A review

of this account at the URL https://www.instagram.com/o0baby on or about October 27, 2022, showed that the images and videos posted to the account were of Dangelo Mckenzie Jr., as compared to the image from Mckenzie's driver's license.

31. Based in part on the information provided above, a search warrant was authorized in the Eastern District of Michigan for the residence on Hazelwood Street in Detroit, Michigan. On March 8, 2023, the FBI executed the search warrant there. Present at the house were Individual A, Individual B, Individual C (Individual B's adult son), and three minor children. Individual B voluntarily spoke with me and told me that Mckenzie had recently moved back into the residence when Individual B found out that he was moving from place to place. Individual B was aware that Mckenzie had spent some time at the recording studio in Warren, Michigan and stated that nobody who resides at the house on Hazelwood Street had spent any time at the studio. The only other person who had been to the studio was Individual A to pick Mckenzie up and bring him home. Prior to the past couple of months of Mckenzie staying there and the time that he was kicked out of the house, Mckenzie would stay at the residence for a few days at a time and with his father at another location in Detroit for a few days at a time.

32. During the execution of the search warrant a Task Force Officer from the Southfield Police Department recognized Dangelo Mckenzie. She provided a police report from January 2021 in which a video of a minor victim (hereafter

referred to as MV2) engaged in sexual acts with a dog was reported by the Principal of the SRAC High School in Southfield. The minor victim, who was 17 at the time with a date of birth in 2003 and who resides in the Eastern District of Michigan, was interviewed after she was identified. During the interview she stated that since approximately January 2020, one year prior, she had been getting notices from Snapchat that she had been logged out. She then started receiving text messages and phone calls from numbers she did not recognize and that the individual contacting her had nude images and videos of her. The unknown individual threatened to release the images and videos if she did not send more.

33. MV2 was instructed to log into a different Snapchat account and send nude photos of herself. MV2 was instructed how to pose in the photos. The individual then contacted her again demanding additional videos. When MV2 stopped responding the individual posted a video of MV2 performing a sex act with a dog.

34. MV2 suspected the unknown individual was her ex-boyfriend Dangelo Mckenzie. She was aware that other females had told her Mckenzie was hacking into their accounts. MV2 had dated Mckenzie and had provided him with her Apple iCloud login information.

35. MV2 knew there was a method to identify IP addresses of individuals

logging into Snapchat. When she checked the Snapchat IP log she recognized the IP address logging into it as Mckenzie's IP address.

36. An extraction of MV2's iPhone identified multiple message threads from VOIP phone numbers that corroborated the statements made by MV2.

37. The conversations I observed between AV1 and Mckenzie over VOIP are consistent with the conversations that were reported to Southfield by MV2. The conversations that occurred with MV2 also occurred over VOIP and included a similar pattern of threatening behavior. Based on this information and the fact that MV2 appeared to recognize Mckenzie in the conversations, I believe that it was Mckenzie that was in contact with both AV1 and MV2.

CONCLUSION

38. Based on the foregoing, there is probable cause to believe that Dangelo Charles Mckenzie Jr. is in violation of 18 U.S.C. § 2252A(a)(2) (receipt of child pornography), 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), 18 U.S.C. §§ 875(d) (threatening communications) and 2261A(2)(B) (online stalking).

Respectfully submitted,

Matthew Hughes, Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence
and/or by reliable electronic means.

HON. ANTHONY P. PATTI March 8, 2023
UNITED STATES MAGISTRATE JUDGE